Safety-Critical Systems 4:
Engineering of Embedded Software Systems
WiSe 2002/03

Jan Bredereke

due: Oct. 31, 2002

Solution for Assignment 2

Bicycle Odometer – System Requirements Specification

The following specification makes several choices at points where the assignment is not precise. These choices are not marked in the text, even though this was required by the assignment.

This specification restricts itself to behavioural requirements. Non-behavioural requirements such as size and colour of the case, robustness against mechanical shock, resistance against water, form of the electrical plug etc. must be specified elsewhere.

Environmental Quantities

This specification takes the environmental quantities specification by Jan Bredereke for Assignment 1 as a base, which is not repeated here.

Accuracy

The accuracy of the measurement of electrical resistance for ^{m}sensor shall be $\pm 3\ \Omega$.

The accuracy of the measurement of short time intervals (< 1 s) is stated below with the mode class and with one of the auxiliary functions.

The accuracy of long time intervals (≥ 1 s), i.e., the clock drift, shall be $\pm 10^{-3}$ of the true value. This shall hold for any sub-interval of time.

Conditions

name	condition
^{p}sensorClosed	^{m}sensor $< 10\ \Omega$
^{p}magnetAway	Drtn($\neg$ ^{p}sensorClosed) ≥ 10 ms
^{p}buttonPressed	Drtn(^{m}button $=$ ^{C}down) ≥ 10 ms
^{p}buttonPressedShort	0 s $<$ Drtn(^{p}buttonPressed) $<$ 2 s
^{p}buttonPressedLong	2 s $\leq$ Drtn(^{p}buttonPressed)

Event Classes

name	event class
^{e}roundComplete	@T(^{p}magnetAway)
^{e}switchMode	@F(^{p}buttonPressed) WHEN(^{p}buttonPressedShort)
^{e}reset	@T(^{p}buttonPressedLong)

Mode Classes

^{Cl}display : ^{Md}speed, ^{Md}total, ^{Md}dayTrip

initial mode: ^{Md}speed

Mode	Event Class	New Mode
^{Md}speed	^{e}switchMode $\vee$ ^{e}reset	^{Md}dayTrip
^{Md}dayTrip	^{e}switchMode	^{Md}total
^{Md}total	^{e}switchMode	^{Md}speed
	^{e}reset	^{Md}dayTrip

maximum delay: 10 ms

Auxiliary Functions

^{f}totalPulses $= \#({}^{e}$roundComplete$)$

^{f}totalDist $=$ Round1$({}^{f}$totalPulses $\cdot$ ^{C}circumference$)$ mod ^{C}numberLimit

^{f}dayTripPulses $= \#({}^{e}$roundComplete$) - \#($Prev$({}^{e}$roundComplete, Last$({}^{e}$reset$)))$

^{f}dayTripDist $=$ Round1$({}^{f}$dayTripPulses $\cdot$ ^{C}circumference$)$ mod ^{C}numberLimit

^{f}pulsePeriod $=$

$p_T : H_1,\ r_T : G$, Normal	
$\#({}^{e}\text{roundComplete}) \geq 2$	Last$({}^{e}$roundComplete$)$ $-$ SecondButLast$({}^{e}$roundComplete$)$
$\#({}^{e}\text{roundComplete}) < 2$	^{C}veryLongPulse

The resolution of time measurement for ^{f}pulsePeriod shall be at least 1 ms.

(Note: the precise semantics of the above tabular expression, and the meaning of the box at the top left, will be explained in the seminar shortly. The left column contains conditions, the right column contains the corresponding values.)

^{f}speedRaw $=$ Round$(3.6 \frac{\text{km/h}}{\text{m/s}} \frac{{}^{C}\text{circumference}}{{}^{f}\text{pulsePeriod}})$

^{f}speedDisp $=$

$p_T : H_1,\ r_T : G$, Normal	
${}^{f}\text{pulsePeriod} < 3.6 \frac{\text{km/h}}{\text{m/s}} \frac{{}^{C}\text{circumference}}{1\ \text{km/h}}$	^{f}speedRaw
${}^{f}\text{pulsePeriod} \geq 3.6 \frac{\text{km/h}}{\text{m/s}} \frac{{}^{C}\text{circumference}}{1\ \text{km/h}}$	0 km/h

Note: the above cut-off at 1 km/h avoids the problem of a display not always returning to zero during stand-still of the bicycle, which is annoying.

Requirements on the Environment (NAT)

Monitored Variables

^{f}pulsePeriod $> \frac{1}{39\ \text{s}}$

There are more constraints on the timing and on the speed of the bicycle, which are documented in the specification of the environmental quantities. It is not possible to check them here using the monitored variables themselves, due to the restictions of the sensor and the button.

Controlled Variables

No constraints by the environment.

Requirements on the System (REQ)

^{c}modeInd =

$p_T : H_1$, $r_T : G$, Normal	
inmode(^{Md}speed)	"km/h"
inmode(^{Md}dayTrip)	"km trip"
inmode(^{Md}total)	"km total"

^{c}number =

$p_T : H_1$, $r_T : G$, Normal	
inmode(^{Md}speed)	^{f}speedDisp
inmode(^{Md}dayTrip)	^{f}dayTripDist
inmode(^{Md}total)	^{f}totalDist

Note: in ^{Md}speed mode, no decimal point is displayed, and the number is displayed flush right. If the speed is zero, a single 0 is displayed. Leading zeroes are not displayed. When displaying distances, a decimal point is displayed left of the rightmost digit. The two digits immediately left and right of the decimal point are always displayed, even if they are 0. Otherwise, leading zeroes are not displayed.

Tolerance

The update delay for ^{c}modeInd and ^{c}number must be less than 0.1 s, including the delay by the optical LCD component.

Dictionary

Constants

name	**value**	**description**
^{C}circumference	0.711 m	Circumference of the wheel.
^{C}numberLimit	10000.0	Smallest number which is too large to display.
^{C}veryLongPulse	1000 s	This inter-pulse time means "very long" and will result in a speed display of 0 km/h.

Mathematic Functions

$\mathrm{SecondButLast}(e) = \mathrm{Last}(e, \mathrm{Last}(e))$

$\mathrm{Round} : \mathbb{R}_0^+ \mapsto \mathbb{N}, \qquad \forall x \in \mathbb{R} \,.\, -0.5 \le x - \mathrm{Round}(x) < 0.5$

$\mathrm{Round1} : \mathbb{R}_0^+ \mapsto \mathbb{R}_0^+, \qquad \forall x \in \mathbb{R} \,.\, \mathrm{Round1}(x) = \mathrm{Round}(10\,x)/10$

The other mathematic functions are standard and are interpreted as in the lecture.

Expected Changes

Any implementation should prepare for expected changes by encapsulating them into a single module, if possible. We envisage the following expected changes:

For a larger market, it may be advantageous to let the user select the circumference of the wheel at power-up.

For world-wide selling, it may be advantageous that the user can select the imperial measures miles per hour and miles. This could be done together with the selection of the wheel circumference, when the odometer is extended.

When using a larger display, it may become possible to display all three values simultaneously.

There are other interesting values which can also be computed and displayed: average speed since last stand-still, average speed since the last reset event, not counting stand-still times, maximum speed since the last reset event, absolute current time and date (after suitable initialization), rotation frequency of the pedals (using a second sensor), ... – All these ideas already have been implemented by competitors.